



Subscriber Agreement für AlphaSSL-Zertifikate (EMEA)

Version 1.3

BITTE LESEN SIE DIESEN VERTRAG SORGFÄLTIG DURCH, BEVOR SIE DAS AN SIE ODER IHRE ORGANISATION AUSGESTELLTE DIGITALE ZERTIFIKAT VERWENDEN. DURCH DIE VERWENDUNG DES DIGITALEN ZERTIFIKATES STIMMEN SIE DER EINHALTUNG DER BEDINGUNGEN DIESES VERTRAGES ZU. WENN SIE DEN BEDINGUNGEN DIESES VERTRAGES NICHT ZUSTIMMEN, GEBEN SIE DAS DIGITALE ZERTIFIKAT UMGEHEND ZURÜCK ODER STORNIEREN SIE DEN AUFTRAG INNERHALB VON 7 TAGEN NACH AUSSTELLUNG DES ALPHASSLS GEGEN RÜCKERSTATTUNG DES KAUFPREISES. WENN SIE PROBLEME BEIM VERSTÄNDNIS DIESER VEREINBARUNG HABEN, SCHICKEN SIE UNS BITTE EINE E-MAIL AN legal@globalsign.com

Dieses AlphaSSL Subscriber Agreement (“Vertrag”) gilt ab dem Datum der Anwendung eines digitalen Zertifikates (dem „Gültigkeitsdatum“) zwischen GlobalSign („AlphaSSL CA“) und der Organisation, die das verschlüsselte digitale Zertifikat erhält („Abonnent“).

Die CPS (Zertifizierungspraxiserklärung) der AlphaSSL CA ist durch Verweis hierin aufgenommen und steht unter www.alphassl.com/repository zur Verfügung.

1. Definitionen

Digitales Zertifikat

Eine Ansammlung elektronischer Daten bestehend aus einem öffentlichen Schlüssel zur Identifizierung von Informationen über den Eigentümer des öffentlichen Schlüssels und Gültigkeitsinformationen, die von AlphaSSL CA digital unterzeichnet wurden. Zertifiziert soll sich auf die Tatsache beziehen, dass von AlphaSSL CA ein gültiges, digitales Zertifikat ausgestellt wurde und dass das Digitale Zertifikat nicht widerrufen wurde.

Liste der widerrufenen Zertifikate („CRL“)

Eine Ansammlung elektronischer Daten, die Informationen bezüglich widerrufenen Digitaler Zertifikate enthalten.

Zertifizierungsbehörde („CA“)

Die AlphaSSL CA oder eine Einheit, die von AlphaSSL CA für die Ausgabe Digitaler Zertifikate an Benutzer in einer digitalen Zertifikateshierarchie zertifiziert ist. AlphaSSL CA ist die CA des Abonnenten hierunter.

Digitale Signatur

Die mit einem privaten Schlüssel verschlüsselte Information, die an elektronische Daten angehängt wird, um den Eigentümer des privaten Schlüssels zu identifizieren und die Integrität der elektronischen Daten zu überprüfen. Digital signiert soll sich auf elektronische Daten beziehen, an die eine digitale Signatur angehängt wurde.

Privater Schlüssel

Ein mathematischer Schlüssel, der vom Eigentümer vertraulich behandelt wird und der zur Erstellung digitaler Signaturen oder zur Verschlüsselung elektronischer Daten verwendet wird.

Öffentlicher Schlüssel

Ein mathematischer Schlüssel, der öffentlich zugänglich ist und verwendet wird, um die mit dem passenden privaten Schlüssel erstellten digitalen Signaturen zu überprüfen und elektronische Daten zu verschlüsseln, die nur mit dem passenden privaten Schlüssel entschlüsselt werden können.

Sichere Server-Hierarchie

Eine Sammlung aus CAs und ihrer zertifizierten Benutzer

Abonnent

Eine Einzelperson oder eine Organisation, die bei der CA die Ausstellung eines digitalen Zertifikates beantragt hat

2. Berechtigung zur Verwendung eines digitalen Zertifikates

Gewähren einer Berechtigung

Zum Gültigkeitsdatum gewährt AlphaSSL hiermit dem Abonnent die Genehmigung für den in Abschnitt 8 festgelegten Zeitraum zur Nutzung des eingeschlossenen digitalen Zertifikates zum Erstellen digitaler Signaturen oder zur Verwendung des digitalen Zertifikates in Verbindung mit Bedienungen mit privatem oder öffentlichem Schlüssel.

Berechtigungsbeschränkungen

Der Abonnent darf das digitale Zertifikat nur in Verbindung mit ordnungsgemäß lizenzierte, kryptografischer Software verwenden.

3. Die von AlphaSSL CA bereitgestellten Dienste

Nach der Ausführung dieses Vertrages und der Zahlung aller angefallenen Gebühren, muss AlphaSSL CA oder ein von AlphaSSL CA ernannter Drittanbieter neben der Gewährung der Berechtigung gemäß Abschnitt 2 dem Abonnenten die folgenden Dienstleistungen bereitstellen:

CRL-Verfügbarkeit

Angemessene Anstrengungen müssen unternommen werden, um allen CAs und zertifizierten Benutzern in der Secure Server Hierarchy (i) die aktuelle CRL von AlphaSSL CA und (ii) die von den CAs an AlphaSSL CA bereitgestellten CRLs zusammenzustellen, zu aggregieren und elektronisch verfügbar zu machen; vorausgesetzt, dass AlphaSSL CA seinerseits nicht gegen seine Verpflichtungen hierunter infolge einer Leistungsverzögerung oder eines Leistungsausfalls verstößt, der aus einem Anlagenausfall oder einer Störung des Fernmeldewesens entsteht und den AlphaSSL CA nicht zu verantworten hat.

Widerrufsstatusdienste

Angemessene Anstrengungen müssen unternommen werden, um den CAs, zertifizierten Benutzern und Benutzern solcher digitaler Zertifikate in der Secure Server Hierarchy Informationen hinsichtlich des Status bestimmter digitaler Zertifikate zur Verfügung zu stellen; vorausgesetzt, dass AlphaSSL CA ihrerseits nicht gegen ihre Verpflichtungen hierunter infolge einer Leistungsverzögerung oder eines Leistungsausfalls verstößt, der aus einem

Anlagenausfall oder einer Störung des Fernmeldewesens entsteht und den AlphaSSL CA nicht zu verantworten hat.

Site-Seal

AlphaSSL CA erlaubt Antragstellern die Verwendung des AlphaSSL CA Site-Seals auf der Website des Antragstellers mit einer maximalen täglichen Rate von 500.000 [fünfhunderttausend] Abrufen pro Tag. AlphaSSL CA behält sich das Recht vor, die Verfügbarkeit dieses Seals zu beenden, sollte diese Grenze überschritten wird.

Widerrufen digitaler Zertifikate

AlphaSSL CA wird ein ausgestelltes AlphaSSL-Zertifikat bei Eintritt eines der folgenden Ereignisse widerrufen:

- Der Abonnent beantragt den Widerruf seines AlphaSSL-Zertifikates
- AlphaSSL CA erhält begründete Beweise, dass der private Schlüssel des Abonnenten (entsprechend dem öffentlichen Schlüssel im AlphaSSL-Zertifikat) beeinträchtigt oder dass das AlphaSSL-Zertifikat anderweitig missbraucht wurde
- AlphaSSL CA erhält Bescheid oder erlangt anderweitig Kenntnis, dass ein Abonnent gegen eine seiner wesentlichen Verpflichtungen gemäß dem Subscriber Agreement verstößt
- AlphaSSL CA erhält Bescheid oder erlangt anderweitig Kenntnis, dass ein Abonnent ein Zertifikat für kriminelle Aktivitäten, wie z.B. Phishing-Attacken, Betrug, etc. verwendet
- AlphaSSL CA erhält Bescheid oder erlangt anderweitig Kenntnis, dass ein Gericht oder Vermittler das Recht eines Abonnenten zur Verwendung des im AlphaSSL-Zertifikates aufgelisteten Domainnamens widerrufen hat oder dass der Abonnent versäumt hat, seinen Domainnamen zu verlängern
- AlphaSSL CA erhält Bescheid oder erlangt anderweitig Kenntnis über eine wesentliche Änderung der im AlphaSSL-Zertifikat enthaltenen Informationen
- Eine Festlegung im eigenen Ermessen von AlphaSSL CA, dass das AlphaSSL-Zertifikat nicht gemäß den AlphaSSL-Richtlinien von AlphaSSL CA ausgestellt wurde
- Falls AlphaSSL CA beschließt, dass eine der im AlphaSSL-Zertifikat angezeigten Informationen nicht richtig ist
- AlphaSSL CA stellt aus irgendeinem Grund den Betrieb ein und hat nicht dafür gesorgt, dass eine andere AlphaSSL CA einen Widerrufungs-Support für das AlphaSSL-Zertifikat bereitstellt
- Das Recht von AlphaSSL CA auf Ausstellung von AlphaSSL-Zertifikaten läuft aus oder wird widerrufen oder beendet [sofern AlphaSSL CA keine Absprachen trifft, den Aufbewahrungsort der CRL/OCSP zu pflegen]
- Der private Schlüssel von AlphaSSL CA für die Ausstellung seiner AlphaSSL-Zertifikate wurde beeinträchtigt
- AlphaSSL CA erhält Bescheid oder erlangt anderweitig Kenntnis, dass ein Abonnent als abgewiesene Partei oder unerlaubte Person auf eine schwarze Liste gesetzt wurde oder von einem untersagten Bestimmungsort gemäß dem Gerichtsstand von AlphaSSL CA am Betriebsort agiert
- Die kontinuierliche Nutzung des Zertifikates ist für das AlphaSSL CA Trust-Modell nachteilig

Sollte sich herausstellen, dass die Zertifikatesnutzung für AlphaSSL CA nachteilig ist, berücksichtigt AlphaSSL CA u.a. Folgendes:

- Die Art und Anzahl der eingegangenen Beschwerden
- Die Identität des/der Beschwerdeführer(s)
- Sachdienliche, gültige Rechtsvorschriften
- Antworten des Abonnenten auf die angebliche nachteilige Verwendung

4. Verpflichtungen des Abonnenten

Dieses Subscriber Agreement nennt eigens Microsoft als ausdrücklichen Drittbegünstigten. Als solcher garantiert und vereinbart der Abonnent mit GlobalSign und allen Zertifikatesempfängern Folgendes:

Datengenauigkeit

Der Abonnent verpflichtet sich, AlphaSSL CA jederzeit genaue und vollständige Informationen zur Verfügung zu stellen, und zwar sowohl in der AlphaSSL-Zertifikatesanfrage von AlphaSSL CA als auch, wenn von AlphaSSL CA nicht anders gefordert, im Zusammenhang mit der Ausstellung des/der digitalen AlphaSSL-Zertifikates von AlphaSSL CA, das von AlphaSSL CA zur Verfügung gestellt wird.

Der Abonnent muss auch von der Einreichung jeglicher Materialien an AlphaSSL CA oder ein anderes AlphaSSL CA-Verzeichnis, die Äußerungen enthalten, die gegen ein Gesetz oder die Rechte einer Partei verstoßen, Abstand nehmen.

Schlüsselerstellung

Gemäß dem AlphaSSL CA-Modell nutzt der Abonnent ein zuverlässiges System, um seine eigenen privaten-öffentlichen Schlüssel zu erstellen, wobei auch die folgenden Bedingungen gelten:

- (a) Der Abonnent erstellt Abonnentenschlüssel mithilfe eines Algorithmus, der für den Zweck elektronischer Signaturen als geeignet gilt
- (b) Der Abonnent verwendet eine Schlüssellänge und einen Algorithmus, der für den Zweck elektronischer Signaturen als geeignet gilt

Schutz des privaten Schlüssels

Der Abonnent oder ein Subunternehmer (z.B. Hosting-Anbieter) unternimmt alle notwendigen Maßnahmen zur Aufrechterhaltung der alleinigen Kontrolle, vertraulichen Behandlung und zum ordnungsgemäßen und kontinuierlichen Schutz des privaten Schlüssels, der dem öffentlichen Schlüssel entspricht, der im/in den angeforderten AlphaSSL-Zertifikat(en) von AlphaSSL CA (und jeder verbundenen Zugangsinformation oder Einrichtung – z.B. Passwort oder Token) enthalten ist.

Der Abonnent muss sicherstellen, dass der an die AlphaSSL CA eingereichte öffentliche Schlüssel dem verwendeten privaten Schlüssel entspricht.

Der Abonnent muss eine angemessene und zumutbare Sorgfalt walten lassen, um die unautorisierte Nutzung seines privaten Schlüssels zu verhindern.

Annahme des AlphaSSL-Zertifikates von AlphaSSL CA

Der Abonnent darf das/die AlphaSSL-Zertifikat(e) von AlphaSSL CA weder installieren noch verwenden, solange es/sie nicht geprüft und die Richtigkeit der Daten in jedem AlphaSSL-Zertifikat von AlphaSSL CA bestätigt wurden.

Verwendung des AlphaSSL-Zertifikates von AlphaSSL CA

Der Abonnent darf das AlphaSSL-Zertifikat von AlphaSSL CA nur auf dem Server installieren, der unter dem auf dem AlphaSSL-Zertifikat von AlphaSSL CA aufgelisteten Domainnamen zugänglich ist, und das AlphaSSL-Zertifikat von AlphaSSL CA ausschließlich in Übereinstimmung mit allen anwendbaren Gesetzen, bis zur Anzahl der vereinbarten Serverlizenzen, für autorisierte Unternehmensgeschäfte und ausschließlich gemäß dem Subscriber Agreement zu verwenden.

Meldepflicht und Widerruf

Der Abonnent verpflichtet sich, umgehend die Verwendung eines AlphaSSL-Zertifikates von AlphaSSL CA und des verbundenen privaten Schlüssels zu beenden und umgehend den Widerruf des AlphaSSL-Zertifikates von AlphaSSL CA zu beantragen, falls:

- Ein Verlust, Diebstahl, eine Veränderung, unautorisierte Offenlegung oder eine andere Gefährdung des privaten Schlüssels seitens des Zertifikatessubjekts vorliegt
- Der Abonnent anzeigt, dass die ursprüngliche AlphaSSL-Zertifikatsanfrage nicht autorisiert war und rückwirkend keine Autorisierung erteilt wird
- Das Zertifikatessubjekt oder sein ernannter Abonnent gegen eine wesentliche Verpflichtung der CPS verstößt
- Die Erfüllung der Verpflichtungen einer Person gemäß der CPS verzögert oder von einer natürlichen Katastrophe, einem Computer- oder Fernmeldeausfall oder einer anderen Ursache, die die Person nicht zu verantworten hat, verhindert wird, und infolge dessen die Informationen einer anderen Person wesentlich bedroht oder gefährdet werden
- Eine Veränderung der im Zertifikat des Zertifikatessubjekts enthaltenen Information erfolgte
- Dieses Subscriber Agreement gekündigt wurde
- Die Zuordnung zwischen einem Unternehmenskunden und einem Abonnenten wird festgelegt oder anderweitig beendet
- Die Information innerhalb des Zertifikates, mit Ausnahme der nicht verifizierten Abonnenteninformation, fehlerhaft ist oder geändert wurde

Beendigung der Nutzung des AlphaSSL-Zertifikates

Der Abonnent muss die Nutzung des privaten Schlüssels gemäß dem im AlphaSSL-Zertifikat von AlphaSSL CA aufgelisteten Schlüssel umgehend beenden, sobald das AlphaSSL-Zertifikat von AlphaSSL CA abgelaufen ist oder widerrufen wird.

5. Genehmigung zur Veröffentlichung der Informationen

Der Kunde stimmt zu, dass AlphaSSL CA die Seriennummer des kundeneigenen digitalen Zertifikates in Verbindung mit der Verbreitung von Statusinformationen zu CRLs und zum digitalen Zertifikat innerhalb und außerhalb der AlphaSSL CA Secure Server Hierarchy veröffentlichen darf.

6. HAFTUNGSAUSSCHLUSS UND HAFTUNGSBEGRENZUNG IN KEINEM FALL (AUSSER BEI BETRUG ODER FAHRLÄSSIGEM FEHLVERHALTEN) IST ALPHASSL CA FÜR INDIREKTE ODER FOLGESCHÄDEN ODER SCHADENERSATZZAHLUNGEN, ODER FÜR GEWINN- ODER DATENVERLUST ODER ANDERE INDIREKTE ODER FOLGESCHÄDEN ODER SCHADENERSATZZAHLUNGEN VERANTWORTLICH, DIE IM ZUSAMMENHANG MIT DER VERWENDUNG, LIEFERUNG, LIZENZ, ERFÜLLUNG ODER

NICHTERFÜLLUNG VON ZERTIFIKATEN, DIGITALEN SIGNATUREN ODER JEDLICHEN ANDEREN TRANSAKTIONEN ODER DIENSTLEISTUNGEN, DIE VON DER CPS ANGEBOTEN ODER IN ERWÄGUNG GEZOGEN WERDEN, ENTSTANDEN SIND, MIT AUSNAHME VON SCHÄDEN, DIE (GEMÄSS DER CPS) AUS DEM VERTRAUEN AUF DIE GEPRÜFTE INFORMATION ZUM ZEITPUNKT DER AUSSTELLUNG DES ZERTIFIKATES IN EINEM SECURE SERVER-ZERTIFIKAT BIS ZU EINEM BETRAG VON 1000 USD ENTSTANDEN SIND. ALPHASSL CA IST IN DIESEM FALL NICHT HAFTBAR, FALLS DER FEHLER IN DIESER GEPRÜFTEN INFORMATION AUF EINEN BETRUG ODER FAHRLÄSSIGES FEHLVERHALTEN DES ANTRAGSTELLERS ZURÜCKZUFÜHREN IST. ALPHASSL CA IST IN DIESEM FALL NICHT HAFTBAR, FALLS DER BENUTZER SEINE IN DER CPS UND IN DIESEM VERTRAG GENANNTE VERPFLICHTUNGEN NICHT EINHÄLT.

7. Laufzeit und Kündigung

Dieser Vertrag endet frühestens:

7.1 Ein Jahr, zwei, drei, vier oder fünf Jahre ab dem Gültigkeitsdatum (je nach Gültigkeit des Zertifikates);

7.2 Nach dem Versäumnis des Abonnenten, seinen wesentlichen Verpflichtungen gemäß diesem Vertrag nachzukommen, wenn ein solcher Verstoß nicht innerhalb von dreißig (30) Tagen nach Eingang der Benachrichtigung hiervon von AlphaSSL CA behoben ist;

8. Auswirkung der Kündigung

Bei Kündigung dieses Vertrages aus irgendeinem Grund wird das digitale Zertifikat des Abonnenten von AlphaSSL CA gemäß den zu dem Zeitpunkt gültigen Vorgehensweisen von AlphaSSL CA widerrufen. Bei Widerruf des AlphaSSL-Zertifikates von AlphaSSL des Abonnenten aus irgendeinem Grund, enden alle dem Abonnenten gemäß Abschnitt 2 gewährten Befugnisse. Eine solche Kündigung oder ein solcher Widerruf wirkt sich nicht auf die Abschnitte 5, 6, 7, 9 und 10 dieses Vertrages aus, die im erforderlichen Maße für die vollständige Erfüllung hiervon vollständig gültig und wirksam bleiben sollen.

9. Sonstige Bestimmungen

Anwendbares Recht

Diese Vereinbarung unterliegt den Gesetzen in Belgien und soll gemäß diesen Gesetzen ausgelegt und interpretiert werden, ungeachtet seiner Bestimmungen bezüglich der Kollision von Gesetzen. Ausschließlicher Gerichtsstand ist Leuven.

Bindende Wirkung

Sofern nicht anderweitig vorgesehen ist diese Vereinbarung bindend und wirkt zugunsten der Parteien und ihrer Rechtsnachfolger und -vertreter der Parteien. Weder dieser Vertrag noch das digitale Zertifikat des Abonnenten ist vom Abonnenten abtretbar. Jede besagte Übertragung oder Abtretung ist ungültig und wirkungslos und berechtigt AlphaSSL CA, diesen Vertrag zu kündigen.

Trennbarkeit

Wenn eine Bestimmung dieses Vertrages oder deren Anwendung aus irgendeinem Grund oder in irgendeinem Maße ungültig oder nicht durchsetzbar sein sollte, werden der restliche Vertrag

und die Anwendung einer solchen Bestimmung für andere Personen oder Umstände so ausgelegt werden, dass sie die Absicht der Parteien bestmöglich wiedergeben.

ES WIRD AUSDRÜCKLICH VERSTANDEN UND AKZEPTIERT, DASS JEDE EINZELNE BESTIMMUNG DIESES VERTRAGES, DIE EINE HAFTUNGSBEGRENZUNG, EINEN HAFTUNGSAUSSCHUSS ODER DEN AUSSCHLUSS VON SCHÄDEN GEWÄHRLEISTET, VON DEN PARTEIEN ALS UNABHÄNGIG UND GETRENNT VON ALLEN ANDEREN BESTIMMUNGEN GESEHEN UND ALS SOLCHES ERZWUNGEN WERDEN MUSS.

Gesamter Vertrag

Dieser Vertrag stellt das gesamte Einverständnis und die Einigung der Parteien im Hinblick auf den Gegenstand dar und ersetzt alle vorhergehenden und gleichzeitigen Schriftstücke oder Einverständnisse der Parteien.

Hinweise

Sobald der Kunde es wünscht oder erfordert, eine Nachricht, Forderung oder Anfrage an AlphaSSL CA bezüglich dieses Vertrages zukommen zu lassen, muss jede solche Mitteilung schriftlich erfolgen und ist nur dann gültig, wenn sie per Kurierdienst, der die Lieferung schriftlich bestätigt, oder per Post mit Einschreiben/Rückschein, Porto im Voraus bezahlt, Rückschein angefordert und an AlphaSSL CA an Globalsign nv/sa, z. Hd. AlphaSSL, Ubicenter, Philipssite 5, 3001 Leuven, Belgien, gesendet wird. Solche Mitteilungen sind ab Eingang wirksam.

Genehmigung zur Verwendung von Drittdatenbanken.

Für natürliche Personen kann GlobalSign Positionen, wie Name, Adresse und andere persönliche Informationen prüfen, die während der Anmeldung für entsprechende Drittdatenbanken bereitgestellt werden. Durch Annahme dieser Bedingungen und Konditionen erklären Sie sich mit der Durchführung solcher Prüfungen einverstanden. Bei der Durchführung dieser Prüfungen können von Ihnen bereitgestellte persönliche Informationen an eingetragene Auskunftstellen offengelegt werden, die eine Kopie dieser Informationen behalten können. Sie können versichert bleiben, dass dieser Vorgang nur der Bestätigung der Identität dient und als solches keine Kreditprüfung durchgeführt wird. Ihre Bonität ist durch diesen Vorgang nicht betroffen.

Handelsnamen, Logos.

Aufgrund dieses Vertrages oder der Erfüllung hiervon erwerben der Abonnent und AlphaSSL CA keinerlei Rechte an Warenzeichen, Markenname, Logo oder Produktbezeichnung der anderen Partei und dürfen diese nicht aus irgendeinem Grund verwenden, sofern nicht schriftlich von der Partei genehmigt, die Eigentümer aller Rechte an solchen Warenzeichen, Markenname, Logo oder Produktbezeichnung ist.

10. HINWEIS

Sie müssen AlphaSSL CA umgehend benachrichtigen, wenn ein Fehler in Ihrem Zertifikat vorliegt. Ohne Reaktion des Abonnenten innerhalb von 7 Tagen nach Eingang, gilt das Zertifikat als angenommen.

Durch Annahme des Zertifikates verpflichtet sich der Abonnent, die Kontrolle über den privaten Schlüssel des Abonnenten zu behalten, ein zuverlässiges System zu verwenden und angemessene Sicherheitsvorkehrungen zu treffen, um dessen Verlust, Offenlegung oder unautorisierte Verwendung zu verhindern.